IN THE CLAIMS

1. (Currently Amended) A method for providing virus protection of a computer system ~~comprising~~ including a central processing unit, a hard disk, a nonvolatile ~~random access~~ memory, an Extensible Firmware Interface, and a basic input and output system, the method comprising the steps of:

modifying a command shell of the Extensible Firmware Interface to include a command that operates to copy ~~the~~ a boot sector of the hard disk to the nonvolatile ~~random access~~ memory;

storing the modified Extensible Firmware Interface in the nonvolatile ~~random access~~ memory;

when the computer system is initialized, copying the boot sector of the hard disk to the nonvolatile ~~random access~~ memory;

reading back the boot sector of the hard disk from the nonvolatile ~~random access~~ memory on each boot to bypass boot sector access of the hard disk during system initialization.

2. CANCELLED

3. CANCELLED

4. (Original) The method recited in Claim 1 further comprising the steps of:

adding a field to a BIOS SETUP portion of the BIOS, that allows a user to enable or disable reading the boot record from nonvolatile ~~random access~~ memory on boot;

running the BIOS SETUP portion of the BIOS; and

enabling or disabling reading the boot record from nonvolatile ~~random access~~ memory on boot.

5. (Currently Amended) The method recited in Claim 1 further comprising the steps of:

further modifying the command shell of the Extensible Firmware Interface to include ~~a command~~ a security signature field;

during execution of the Extensible Firmware Interface, displaying the security signature input field to a user; and

~~inputting~~ receiving the required signature prior to updating the stored boot sector.

6. (Currently Amended) The method recited in Claim 4 further comprising the steps of:

further modifying the command shell of the Extensible Firmware Interface to include ~~a command~~ a security signature input field;

during execution of the Extensible Firmware Interface, displaying the security signature input field to a user; and

~~inputting~~ receiving the required signature prior to updating the stored boot sector.

7. (Original) The method recited in Claim 1 wherein the modified Extensible Firmware Interface is stored in a read-only memory.

8. (Original) The method recited in Claim 1 wherein the modified Extensible Firmware Interface is stored in a flash memory.

9. (New) A system for providing virus protection, comprising:

a processor; and

a memory, coupled to the processor, the memory maintaining instructions that when executed by the processor, cause the processor to:

modify a command shell of an Extensible Firmware Interface to include a command that operates to copy a boot sector of a hard disk to the memory,

store the modified Extensible Firmware Interface in the memory,

copy the boot sector of the hard disk to the memory when the system is initialized,

read back the boot sector of the hard disk from the memory on each boot to bypass boot sector access of the hard disk during system initialization.

10. (New) The system of Claim 9, wherein the memory further includes instructions that when executed by the processor, cause the processor to:

add a field to a setup portion of BIOS that allows a user to enable or disable reading of the boot record from memory;

run the setup portion of the BIOS; and

enable or disable reading of the boot record from memory on boot.

11. (New) The system of Claim 9, wherein the memory further includes instructions that when executed by the processor, cause the processor to:

further modify the command shell to include a security signature input field;

display the security signature input field to a user during execution of an Extensible Firmware Interface; and

receiving the security input prior to updating the stored boot sector.

12. (New) The system of Claim 10, wherein the memory further includes instructions that when executed by the processor, cause the processor to:

Further modify the command shell to include a security signature input field;

Display the security signature input field to a user during execution of an Extensible Firmware Interface; and

Receiving the security input prior to updating the stored boot sector.

13. (New) The system of Claim 9, wherein the Extensible Firmware Interface is stored in a read-only memory.

14. (New) The system of Claim 9, wherein the Extensible Firmware Interface is stored in a flash memory.